Policy Privacy

Iniziativa Cube S.r.l.

1. PREMESSA

1.1 Scopo del documento e sintesi dei contenuti

La presente Policy recepisce le disposizioni introdotte dal nuovo Regolamento Generale sulla protezione dei dati personali (UE) 2016/679 (qui di seguito anche "GDPR"), in modo da definire dei requisiti minimi su tematiche relative alla protezione dei dati.
L'obiettivo della presente Global Policy è quello di assicurare un'applicazione omogenea e coerente a livello societario e nei rapporti tra le stessa con terzi dei requisiti dettati dal GDPR.

La presente Rule si applica alla Società, ai membri di organi strategici, di controllo ed esecutivi, ai dipendenti, agli agenti collegati, di seguito indicati come "Dipendenti" (inclusi tutte le persone legate da un contratto di lavoro, quali, ad esempio, dipendenti a tempo determinato, candidati, apprendisti, tirocinanti, stagisti e consulenti esterni).

1.2 Contesto normativo esterno di riferimento

Il GDPR ha l'obiettivo di realizzare parità di condizioni ("*level playing field*") all'interno dell'Unione Europea, in merito al trattamento dei Dati Personali delle persone fisiche (vale a dire Clienti e Dipendenti), incluse ditte individuali e liberi professionisti, a prescindere dalla nazionalità o residenza. Il GDPR non si applica al trattamento dei dati personali relativi a persone giuridiche, inclusi il nome, la forma giuridica ed i suoi dati di contatto.
Il GDPR si applica ai clienti, fornitori e dipendenti, inclusi ditte individuali e liberi professionisti, a prescindere dalla nazionalità o residenza, in relazione a trattamenti dei rispettivi dati personali. Il GDPR non si applica a trattamenti di dati personali di persone giuridiche, inclusi il nome, la forma giuridica ed i contatti.

Inoltre, il GPDR ha un approccio espansivo, prevedendo l'applicazione extraterritoriale delle previsioni ivi contenute.

l GDPR sarà direttamente applicabile negli Stati Membri dell'Unione Europea dal 25 Maggio 2018, senza la necessità di una trasposizione in differenti leggi nazionali.

1.3 Glossario e Acronimi

Parola chiave	Definizione
Società	INIZIATIVA CUBE SRL (di seguito anche "INIZIATIVA")
Dati Personali	Qualunque informazione relativa ad una persona fisica identificata o identificabile ("Interessato")
Persona Fisica	Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Interessato	Persona Fisica (Clienti, Fornitore, Dipendenti) inclusi ditte individuali e liberi professionisti
Categorie Particolari di Dati Personali	Dati personali che rilevino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
Trattamento	Operazione o insieme di operazioni che sono eseguite su dati personali o su insieme di dati personali, tramite mezzi automatizzati o manuali, come ad esempio: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o alterazione, recupero, consultazione, uso, divulgazione per trasmissione, disseminazione o renderli disponibili, allineamento o combinazione, restrizione,

	cancellazione o distruzione.
Titolare del Trattamento	La persona fisica o giuridica, l'autorità pubblica, l'ente o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri
Responsabile del Trattamento	La persona fisica o giuridica, l'autorità pubblica, l'ente o altro organismo che tratta dati personali per conto del Titolare del Trattamento;
Decisione di Adeguatezza	Decisione adottata dalla Commissione Europea per determinare se un Paese extra-EU offre un adeguato livello di protezione dei dati
Terzo	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
Consenso dell'Interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
Periodo di Conservazione Obbligatorio	Il periodo di conservazione è il limite specifico di conservazione dei dati per i trattamenti di dati personali (ad esempio periodi di prescrizione generali e speciali previsti dalle leggi locali, periodi massimi di conservazione stabiliti dai Regulator locali per categorie speciali di informazioni/ documenti, limiti di conservazione richiesti dalle Autorità di Controllo locali con riferimento a determinate finalità di trattamento). Di conseguenza, è il periodo di tempo massimo per conservare legittimamente i dati personali in base al principio di limitazione della conservazione.
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
Violazione dei Dati Personali (c.d. Personal Data Breach)	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
Autorità di Controllo	L'autorità pubblica indipendente istituita da uno Stato membro responsabile del monitoraggio dell'applicazione del GDPR
Protezione dei dati fin dalla progettazione (c.d Data Protection by Design)	Specifiche misure di sicurezza dovrebbero essere prese in considerazione e implementate nello sviluppo di nuovi software / applicazioni ICT / altre risorse finalizzati al trattamento dei dati personali
Protezione dei dati per impostazione predefinita (c.d. Data Protection by Default)	Specifiche misure di sicurezza dovrebbero essere implementate per la protezione dei dati personali trattati e archiviati da software / applicazioni / altre risorse IT esistenti
Acronimo	**Definizione**
DPO	Data Protection Officer

GDPR	General Data Protection Regulation

2. PRINCIPI E REGOLE SOCIETARIE

2.1 Principi Generali per il Trattamento dei Dati

La Società, nel trattare i Dati Personali deve conformarsi ai seguenti principi:

- **Liceità, Correttezza e Trasparenza:** i Dati Personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato.
- **Limitazione della Finalità:** i Dati Personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.
- **Minimizzazione dei Dati**: i Dati Personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
- **Esattezza**: i Dati Personali devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
- **Limitazione della Conservazione:** i Dati Personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.
- **Integrità e Riservatezza**: i Dati Personali devono essere trattati in modo da garantire un'adeguata sicurezza dei stessi, compresa la protezione - mediante misure tecniche e organizzative adeguate - da trattamenti non autorizzati, illeciti e dalla perdita, dalla distruzione o dal danno accidentali mediante misure tecniche e organizzative adeguate. L'accesso ai dati personali deve avvenire sulla base di appropriati processi autorizzativi basati sul principio del *need to know*. Qualunque altra terza parte che legittimamente ha accesso ai Dati Personali di titolarità della Società, è responsabile di proteggerli e deve essere monitorata per assicurare la conformità alle attuali leggi e regolamenti vigenti.
- **Responsabilizzazione (c.d. *Accountability*)**: il Titolare del Trattamento è responsabile per e deve essere in grado di dimostrare la conformità al GDPR.

2.2 Obblighi Generali

La Società deve conformarsi, in relazione a ciascun argomento trattato nei seguenti paragrafi.

2.2.1 Informativa

In ottemperanza ai principi di correttezza e trasparenza del trattamento dei Dati Personali, la Società deve rendere agli Interessati un'apposita Informativa, a meno che questi ultimi non siano stati già informati.

L'Informativa deve essere inviata in tempo: vale a dire contestualmente al momento in cui i Dati Personali sono ottenuti, ovvero entro un periodo di tempo ragionevole dall'ottenimento degli stessi ed in ogni caso al massimo entro un mese (questo limite deve essere interpretato come limite massimo).

L'Informativa deve essere concisa, chiara, comprensibile e facilmente accessibile, con un linguaggio chiaro e semplice (in particolare, se l'Interessato è un minore). Se l'Informativa è online, può essere utilizzata una versione "a più sezioni" in cui gli Interessati sono informati del trattamento dei propri Dati Personali passo dopo passo. Tale approccio consiste nel fornire le informazioni chiave in una breve informativa, collegando ogni sezione alla versione integrale dell'Informativa tramite appositi link.

2.2.2 Liceità del Trattamento

La Società può trattare i Dati Personali esclusivamente in base ad uno dei sei criteri di liceità elencati qui di seguito.

È opportuno rimarcare che non sussiste una distinzione giuridica tra i predetti sei criteri né una gerarchia fra loro. In altre parole, mentre il consenso si concentra *sull'autodeterminazione* dell'interessato quale motivo di liceità, gli altri criteri, invece, ammettono il trattamento, subordinatamente a garanzie e misure adeguate, in situazioni in cui, a prescindere dal consenso, è opportuno e necessario trattare i dati in un determinato contesto al fine di perseguire una finalità legittima e specifica (ad esempio l'esecuzione di un contratto di cui l'Interessato è parte, l'adempimento di un obbligo legale a cui il Titolare del Trattamento è soggetto).

I sei criteri di liceità sono i seguenti:

i. Consenso, che deve avere le seguenti caratteristiche:

   a. Libero – La Società deve valutare anticipatamente se il consenso implica una effettiva e ponderata scelta dell'Interessato. Di conseguenza, il consenso non può essere considerato libero se gli effetti dello stesso minano la libertà di scelta degli individui.

   b. **Specifico –** è necessario ottenere un consenso separato in relazione a distinti trattamenti di dati personali, assicurando un certo livello di controllo e trasparenza per l'Interessato. In caso di dichiarazione scritta che comprende anche altre tematiche, la richiesta di consenso, dovrebbe essere presentata separatamente da altri termini e condizioni, in modo chiaramente distinguibile.

   c. Informato – l'Interessato deve essere preventivamente informato prima di prestare il proprio consenso; ciò è essenziale per consentire agli stessi di prendere decisioni informate, capire a cosa acconsentono ed esercitare il loro diritto di revoca del consenso.

   d. Non ambiguo – è necessaria una chiara indicazione della volontà dell'Interessato – è pertanto obbligatorio avere un atto affermativo dell'Interessato che denoti un sostanziale accordo al trattamento dei propri dati (il silenzio, le caselle precompilate o l'inattività non costituiscono consenso).

   e. Esplicito – è richiesto in determinate circostanze (vale a dire in casi di trattamento di Categorie Particolari di Dati personali, oppure di trasferimento di Dati Personali verso paesi terzi o organizzazioni internazionali in mancanza di Decisioni di Adeguatezza o di garanzie adeguate, come le clausole contrattuali tipo di protezione dei dati personali adottate dalla Commissione Europea o da altre garanzie specificate dall'art 46 GDPR) in cui emerga un notevole rischio per la protezione dei dati e, di conseguenza, sia opportuno un livello elevato di controllo da parte dell'Interessato.

   f. **Dimostrabile –** in linea con il principio di Accountability, il Titolare del Trattamento deve essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. Di conseguenza, la Società deve implementare procedure atte a dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri Dati Personali.

   g. Revocabile – gli interessati hanno il diritto di revocare il proprio consenso in ogni momento, senza subire pregiudizio (vale a dire senza pagare alcuna commissione o senza riduzioni nel livello del servizio). Il consenso deve essere revocato con la stessa facilità con cui è accordato. La revoca del consenso non pregiudica la legittimità del trattamento basato sul consenso prima della revoca.

ii. Esecuzione di un Contratto con l'Interessato ovvero di misure precontrattuali adottate su richiesta dello stesso.

iii. Adempimento di un obbligo legale al quale è soggetto il Titolare Del Trattamento. Tale obbligo deve essere:

   a. un obbligo di legge dettato dallo Stato Membro oppure dall'Unione Europea, e

   b. un **chiaro e preciso** obbligo, la cui applicazione sia prevedibile per le persone che vi sono sottoposte.

   In breve, l'obbligo legale non deve necessariamente discendere da atto legislativo da parte di un parlamento ma deve essere **"chiaro e preciso**" nel rispetto del principio di proporzionalità

   Protezione di un interesse vitale dell'Interessato o di un'altra persona fisica;

iv. Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

v. Perseguimento di un legittimo interesse del titolare del trattamento o di terzi. In particolare, per considerare il legittimo interesse una base giuridica, occorre eseguire un test di bilanciamento *ex-ante* per valutare che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato.

Secondo il principio di Accountability, il test di bilanciamento tra gli interessi (legittimi) della Società e gli interessi e i diritti fondamentali degli Interessati deve essere svolto dal Titolare del Trattamento in maniera chiara e trasparente. Di conseguenza, la Società deve implementare procedure per dimostrare che tutti gli step necessari siano stati considerati, dal momento che la corretta esecuzione del test di bilanciamento potrebbe essere verificata dalle Autorità di Controllo. Il test di bilanciamento *ex-ante* (in quanto qualificabile come un'attività di consulenza) deve essere svolto dal DPO, sulla base delle informazioni e del supporto del Process Owner.

La Società può basarsi sul legittimo interesse per trattare Dati Personali per finalità di marketing diretto senza la necessità di richiedere il consenso agli Interessati. In questo caso, la rilevanza dovrebbe essere data al contesto del trattamento (ovvero il fatto che esiste già un rapporto tra Titolare e Interessato) ed alle aspettative legittime dell'Interessato (che, per l'appunto, si aspetta di ricevere comunicazioni con finalità di marketing). In aggiunta, il GDPR prevede che il trasferimento di dati personali intra-gruppo *per finalità amministrative interne* – inclusi i Dati Personali di clienti o di dipendenti – può essere considerato legittimo interesse.

2.3 Diritti degli Interessati

Il GDPR rafforza l'insieme di diritti degli Interessati già esistenti (quali diritto di accesso, di opposizione e di rettifica) e ne prevede di nuovi (quali diritto all'oblio, limitazione al trattamento e diritto alla portabilità dei dati).
La Società – in base al principio di trasparenza – deve implementare specifiche procedure per gestire le richieste degli Interessati assicurando che ogni comunicazione ad essa sia prontamente gestita.
Ciò implica che la Società deve almeno:

a. Fornire informazioni all'Interessato sui propri diritti (tramite l'Informativa).
b. Rendere disponibile un template che gli Interessati possono utilizzare per esercitare i propri diritti;
c. Valutare – caso per caso – le richieste degli Interessati;
d. Fornire all'Interessato senza ritardo e, in ogni caso, entro un mese dalla ricezione della richiesta, le informazioni relative alle azioni pianificate per soddisfare la medesima. Tale periodo può essere prorogato – previa comunicazione all'Interessato delle ragioni di tale proroga e dei motivi del ritardo di due mesi, se necessario considerando la complessità ed il numero di richieste ricevute.
e. Informare, in caso di mancato ottemperamento della richiesta, l'Interessato in merito alle ragioni dell'inottemperanza e sulla possibilità di poter proporre un reclamo all'Autorità di Controllo.

Il riscontro alla richiesta degli Interessati può essere fornito con diverse modalità, per iscritto o in formato elettronico (ad esempio tramite il sito web nel caso in cui l'informazione sia indirizzata al pubblico).

Predetto riscontro deve essere fornito all'Interessato gratuitamente.

I paragrafi successivi si focalizzano sugli specifici Diritti dell'Interessato.

2.3.1 Diritto di Accesso

L'Interessato ha il diritto di ottenere dalla Società, in qualità di Titolare del Trattamento, la conferma sull'effettivo trattamento dei propri Dati Personali, ed in caso affermativo, di ottenere l'accesso agli stessi. In tal caso, il Titolare deve fornire una copia dei Dati Personali oggetto di trattamento.

2.3.2 Diritto di Rettifica

L'Interessato ha il diritto di ottenere dalla Società, in qualità di Titolare del Trattamento dei dati, conferma sull'avvenuta rettifica di Dati Personali inesatti. Tenuto conto delle finalità del trattamento, l'Interessato ha, altresì, il diritto di ottenere l'integrazione dei Dati Personali incompleti, anche fornendo una dichiarazione supplementare.

2.3.3 Diritto all'Oblio

L'Interessato, prima della scadenza del Periodo di Conservazione Obbligatorio, ha il diritto di richiedere la cancellazione dei propri Dati Personali:

- Se i Dati Personali non sono più necessari per le finalità per cui sono stati raccolti o trattati.
- In caso di revoca del consenso al trattamento ove non sussista altro fondamento giuridico per il trattamento.

- In caso di opposizione al trattamento basato sul legittimo interesse ove il Titolare non riesca a dimostrare che vi sono ulteriori interessi legittimi prevalente per trattare i dati;
- Se i Dati Personali sono trattati illecitamente;
- Se i Dati Personali devono essere cancellati in ottemperanza ad un obbligo legale previsto dal diritto dell'Unione o dello Stato Membro cui è soggetto il Titolare del Trattamento.

A fronte della richiesta dell'Interessato di diritto all'oblio prima della scadenza del Periodo di Conservazione Obbligatorio, la Società deve:

- Esaminare caso per caso, le ragioni della richiesta;
- Implementare specifiche procedure per cancellare selettivamente, in caso di richiesta legittima, i Dati Personali che la Società non ha più diritto o obbligo di conservare (ad esempio la foto sul portale dei Dipendenti oppure la documentazione relativa al contratto di assicurazione per i clienti).

La Società può respingere la richiesta, se:

- questa è presentata dopo la scadenza del Periodo di Conservazione Obbligatorio e, pertanto, i Dati sono stati già cancellati;
- I Dati Personalidevono essere trattati in conformità ad un obbligo legale previsto a livello Europeo e/o Locale, ovvero in base a relazioni contrattuali e/o ad un'altra base giuridica rilevante;
- I Dati Personali devono essere trattati per la gestione di un precontenzioso/ contenzioso e/o una disputa legale (propria o di una terza parte), iniziata prima della richiesta dell'Interessato;
- I Dati Personali devono essere trattati per investigazioni/ ispezioni poste in essere da funzioni di controllo interne ovvero da Autorità di Controllo (alla cui vigilanza è soggetto il Titolare) avviate prima della richiesta dell'Interessato;
- I Dati Personali devono essere trattati per soddisfare una richiesta di un'Autorità di Controllo nazionale e/o sovranazionale indirizzate alla Società.

2.3.4 Diritto di limitazione al trattamento

L'Interessato può richiedere di limitare il trattamento dei propri Dati Personali e di non eseguire nessuna ulteriore modifica degli stessi, se sussiste almeno una delle seguenti circostanze:

- E' contestata l'accuratezza dei Dati Personali;
- Il Trattamento dei Dati Personali è illecito;
- I Dati Personali non sono più necessari per le finalità del trattamento, ma l'Interessato richiede gli stessi per l'accertamento, l'esercizio o la difesa di un proprio diritto in sede giudiziaria
- In attesa della verifica del test di bilanciamento per il legittimo interesse.

Quando il trattamento è limitato, i Dati Personali possono essere utilizzati, salvo che per la conservazione, dal Titolare solo:

- per l'esercizio e la difesa di un diritto in sede giudiziaria;
- per tutelare i diritti di un'altra persona fisica o giuridica;
- per un interesse pubblico rilevante;
- con il consenso dell'Interessato.

2.3.5 Diritto alla portabilità dei dati

Gli Interessati hanno diritto di ricevere i propri Dati Personali in un formato strutturato, comunemente utilizzato e leggibile e di trasmettere i predetti dati ad un altro Titolare, senza alcun ostacolo. Tale diritto si applica ai trattamenti basati sul consenso o su un contratto quale base giuridica ed effettuati effettuato con mezzi automatizzati. In aggiunta, la portabilità riguarda dati forniti consapevolmente ed attivamente dall'Interessato ed anche dai dati generati dalla sua attività.

La trasmissione di "dati personali oggetto di portabilità" all'Interessato deve essere adeguatamente protetta, tramite l'implementazione di misure tecniche necessarie per assicurare il trasferimento sicuro dei Dati all'Interessato nonché la confidenzialità, integrità degli stessi.

L'esercizio del diritto di portabilità non inficia gli altri diritti (ad esempio, il diritto di accesso).

2.3.6 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

L'Interessato ha il diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, a meno che il predetto trattamento automatizzato non sia:

- Autorizzato da normative dell'Unione Europea o degli Stati Membri a cui il Titolare del Trattamento è soggetto;
- Necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; oppure
- Basato su esplicito consenso dell'Interessato

In tali casi, la Società deve:
- Informare adeguatamente gli Interessati circa le attività di profilazione e le decisioni annesse.
- Informare l'Interessato del suo diritto di:
    - richiedere intervento umano;
    - Esprimere la propria opinione;
    - ottenere una spiegazione sulla decisione; e
    - contestare la decisione.
- Implementare misure idonee per la salvaguardia dei diritti, delle libertà e degli interessi legittimi degli Interessati;
- Usare procedure matematiche o statistiche per la profilazione, implementare misure tecniche ed organizzative per gestire adeguatamente e correggere eventuali imprecisioni e minimizzare il rischio di errore;
- Eseguire la valutazioni d'impatto sulla protezione dei dati.

I processi decisionali basati sulla profilazione non possono riguardare i minori.

2.4 Conservazione dei Dati

Al fine di assicurare la correttezza del trattamento, uno dei requisiti chiave del GDPR è il principio di limitazione della conservazione, in base al quale i Dati Personali non devono essere conservati per un arco di tempo superiore al conseguimento delle finalità per le quali sono stati raccolti, o per cui sono stati ulteriormente trattati

In questa prospettiva la Società deve individuare il periodo massimo di tempo per conservare legittimamente i Dati Personali (c.d. Periodo di Conservazione Obbligatorio), secondo le leggi ed alle normative locali.

Di conseguenza, la Società deve dotarsi di procedure atte a garantire che decorso il Periodo di Conservazione Obbligatorio, i Dati Personali siano cancellati oppure resi anonimi anonimizzati in modo tale che l'Interessato non sia identificato o comunque identificabile in maniera da rendere l'Interessato non più identificabile, così come previsto dalle normative locali.

Il principio di limitazione della conservazione deve essere applicato anche agli archivi cartacei. Di conseguenza, ogni Società del Gruppo deve mappare i propri archivi, identificando sulla base della natura dei documenti, il periodo di conservazione rilevante previsto da leggi e normative locali.

2.4.1 Trattamenti di Dati Personali oltre il Periodo di Conservazione Obbligatorio

I Dati Personali possono essere trattati oltre il Periodo di Conservazione Obbligatorio nel caso in cui si verifichi almeno una delle seguenti circostanze:

- La necessità di continuare a trattare i Dati Personali per la risoluzione di un contenzioso bancario e/o una disputa legale con la Società e/o con Terzi, iniziati prima della scadenza del Periodo di Conservazione Obbligatorio.
- La necessità di continuare a trattare i dati personali per indagini/ ispezioni poste in essere da funzioni di controllo interne e/o Autorità di Controllo (alla cui vigilanza è soggetto il Titolare), iniziate prima della scadenza del Periodo di Conservazione Obbligatorio.
- La necessità di continuare a trattare i Dati Personali per ottemperare alle richieste di Autorità di Controllo nazionale e/o sovranazionale indirizzate alla Società del Gruppo prima della scadenza del Periodo di Conservazione Obbligatorio.

2.4.2 Diritto alla cancellazione dei dati personali pubblicati su Internet

Nel caso in cui la Società abbia pubblicato i Dati Personali su internet (ad esempio sul sito web istituzionale), è obbligata ad:
- accettare la richiesta e procedere alla cancellazione, a meno che non sussista una delle circostanze di cui al Paragrafo 2.4.1;

- Informare (considerando eventuali costi) le terze parti che stanno trattando tali dati dell'obbligo di cancellare eventuali collegamenti, copie o repliche..

La Società del Gruppo è esentata dall'obbligo di cancellazione qualora risulti impossibile o richieda uno sforzo sproporzionato (ad esempio la cancellazione implica dei costi molto elevati e/o è tecnicamente impegnativa per il Titolare del Trattamento). In conformità al principio di Accountability, tale impossibilità deve essere ampiamente documentata.

2.4.3 Obbligo di notifica relativo alla cancellazione

La Società del Gruppo deve comunicare la cancellazione di Dati Personali ad ogni destinatario a cui i Dati Personali cui sono stati trasmessi, a meno che ciò si riveli impossibile o implichi uno sforzo sproporzionato (ad esempio la comunicazione è lunga e/o costosa e/o tecnicamente sfidante per il Titolare). In conformità con il principio di Accountability, tale impossibilità deve essere ampiamente documentata.

2.5 Dati relativi ai Dipendenti

Oltre ai requisiti elencati nei paragrafi precedenti, ciascuna Società del Gruppo deve assicurare la protezione dei diritti e delle libertà dei Dipendenti relativamente al trattamento dei Dati Personali nel rapporto di lavoro.
In particolare, ogni Società del Gruppo deve trattare i Dati Personali dei propri Dipendenti per attività connesse al rapporto di lavoro e solo per finalità specifiche e legittime, in linea con i principi di proporzionalità e necessità.

La società riconosce e rispetta la privacy dei propri Dipendenti limitando la raccolta, l'accesso e l'utilizzo di Dati Personali relativi al rapporto di lavoro.

La raccolta, l'accesso e l'utilizzo di Dati Personali relativi ai Dipendenti sono limitati secondo le leggi e i regolamenti locali.

L'impegno della società di rispettare la privacy dei Dipendenti non è abilita questi ultimi a svolgere inappropriate attività personali sul posto di lavoro (ad es. gli strumenti elettronici aziendali sono destinati esclusivamente ad usi lavorativi quindi l'utilizzo per altri usi dovrebbe essere ridotte al minimo e non dovrebbe influenzare in alcun modo le attività lavorative). La società, inoltre, ha il diritto di avere accesso ai luoghi di lavoro e agli strumenti di lavoro e di prendere visione delle comunicazioni e delle informazioni relative al lavoro, ove necessario, al fine di garantire la sicurezza e la protezione dei propri Sistemi IT, in ogni caso nei limiti consentiti dalla legge applicabile.

2.6 Accountability

I seguenti paragrafi sono incentrati sugli obblighi che la Società deve rispettare (intesi come requisiti minimi) per dimostrare la conformità con i principi della GDPR.

2.6.1 Misure di Sicurezza

La Società deve implementare misure tecniche ed organizzative adeguate ad assicurare e dimostrare che il trattamento sia in linea con i principi del GDPR e per proteggere i dati personali da trattamenti non autorizzati e illeciti.

2.6.2 Protezione dei dati fin dalla progettazione (by Design) e protezione per impostazione predefinita (by Default)

La protezione dei dati fin dalla progettazione (by Design) e protezione per impostazione predefinita (by Default) dovrebbe essere garantita per la sicurezza dei dati personali dal Titolare o dal Responsabile del trattamento che agisce per suo conto. Per ulteriori dettagli, si può far riferimento alla GOR "*Security of Application*".

2.6.3 Trattamenti tramite Terzi (Responsabile del Trattamento)

Se il trattamento dei Dati Personali deve essere eseguito per conto di una parte terza rispetto alla Società, la Terza Parte deve essere nominata Responsabile del Trattamento tramite uno specifico accordo (il c.d. Data Processing Agreement).

Il GDPR impone elevati obblighi alle Società nella selezione dei propri fornitori esterni; più nel dettaglio, il Data Processing Agreement deve essere firmato con i fornitori e deve includere una serie di informazioni (ad esempio la tipologia di dati trattati e la durata del trattamento) e di obblighi (assistenza nel caso di violazioni dei dati personali, misure tecniche e organizzative appropriate e obblighi di assistenza in caso di ispezioni). Inoltre, la Società deve implementare misure *ad-hoc* in caso di:

- Trasferimento di Dati Personali verso paesi non-EU (i.e., al di fuori dello Spazio Economico Europeo), nei casi in cui non siano assicurata un'adeguata protezione per il trasferimento;
- Fornitori che offrono servizi di cloud computing, intesi quali serie di tecnologie e modelli di servizio basati sull'utilizzo di internet e sullo sviluppo di applicativi IT, capacità di elaborazione, archiviazione e spazi di memoria.

2.6.4 Registro Trattamenti

La società deve implementare e manutenere un registro di tutte le attività di trattamento dei Dati Personali effettuati sotto la propria responsabilità, in qualità di Titolare o di Responsabile del Trattamento ("Registro dei Trattamenti"). Il Registro dei Trattamenti è una misura efficace per dimostrare la conformità al principio di Accountability, perché consente una visione di insieme di tutti i trattamenti eseguiti; la Società e ogni sede locale della stessa, come Titolare o Responsabile del Trattamento, deve rendere il Registro dei Trattamenti disponibile all'Autorità di Controllo su richiesta.

2.6.5 Data Protection Officer (DPO)

Il DPO è fondamentale al fine di garantire il principio di Accountability e la sua nomina facilita la conformità ai requisiti del GDPR. Il DPO è obbligatorio solo se le attività principali (core) del Titolare/i (o del Responsabile/i) del Trattamento consistono in:

- trattamenti che, per loro natura, perimetro e/o finalità, richiedono un monitoraggio regolare e sistematico di Interessati su larga scala; e
- trattamenti su larga scala di categorie particolari di dati o di dati relativi a condanne penali e reati

Nel caso di nomina del DPO su base volontaria, i requisiti del GDPR devono essere applicati per la sua nomina, posizione e attività, come se nel caso di designazione obbligatoria.

Nel caso in cui il DPO non sia richiesto o non sia volontariamente nominato, la Società può comunque dotarsi di uno staff per la gestione di attività relative alla protezione dei dati personali. In questo caso, è importante assicurare che non vi sia confusione relativamente a titolo, status, posizione ed attività rispetto a quelle del DPO (quindi, occorre evitare di utilizzare la qualifica DPO).

Una volta nominato, il DPO deve essere coinvolto in tutte le tematiche relative alla protezione dei dati e deve essere in grado di svolgere le proprie attività con un sufficiente grado di autonomia all'interno della propria organizzazione.

Il DPO deve informare il più alto livello di management del Titolare (o Responsabile) per garantire che il senior management sia sempre consapevole del parere e dell'opinione del DPO.

In ogni caso, il DPO garantisce la conformità al GDPR ma non è personalmente responsabile del mancato rispetto di quest'ultimo.

2.6.6 Codici di Condotta

L'adozione di un Codice di Condotta è uno utile strumento dimostrare la conformità al GDPR del Titolare del Trattamento (ovvero del Responsabile). La Società può valutare di aderire a predetti Codici di Condotta approvati dalle rispettive Autorità di Controllo, dal Garante Europeo della Protezione dei Dati (oppure a Codici che hanno validità generale all'interno dell'Unione Europea, confermati da un atto implementativo dalla Commissione Europea.

2.6.7 Certificazioni

L'adesione a meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati ha lo scopo di dimostrare la conformità al GDPR dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento e possono pertanto utilizzati dalla Società.

3. ASSETTO ORGANIZZATIVO

- Il DPO è esternalizzato attraverso:
  - Outsourcing delle attività del DPO ad una parte terza al di fuori delle Società.

La Società nomina un referente interno per interfacciarsi con il DPO.

Il DPO deve informare periodicamente (ad esempio con periodicità annuale) il Consiglio di Amministrazione e/o i comitati Strategici della Società, sulle questioni più rilevanti relative alla protezione dei dati a livello locale.

Il DPO di Iniziativa deve informare periodicamente (ad esempio con periodicità annuale) il Consiglio di Amministrazione /o i i comitati Strategici, fornendo una panoramica dello stato della protezione dei dati.

4. SUDDIVISIONE DELLE RESPONSABILITÀ TRA IL DPO DI GRUPPO E I DPO LOCALI

4.1 Responsabilità del DPO di Gruppo

Il DPO di Iniziativa è responsabile di:
- Emanare linee guida riguardanti la gestione della protezione dei dati;
- Sviluppare Regole determinanti standard minimi per la protezione dei dati e monitorarne e tracciarne l' approvazione, adozione e implementazione;
- Emanare pareri, coordinare e monitorare le tematiche relative alla protezione dei dati e fornire supporto relativamente agli eventi maggiormente critici inerenti la protezione dei dati;
- Definire la metodologia di Data Protection Impact Assessment (DPIA) da seguire;
- Definire la struttura del Registro del trattamento dei dati da implementare;
- Definire i contenuti della formazione (training);
- Ricevere periodici flussi informativi;
- Informare periodicamente (es. annualmente) il Consiglio di Amministrazione e i comitati strategici di Iniziativa.